



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/765,417	01/27/2004	Fujio Watanabe	M-15391 US	2223
32605 7590 01/23/2008 MACPHERSON KWOK CHEN & HEID LLP 2033 GATEWAY PLACE SUITE 400 SAN JOSE, CA 95110			EXAMINER PATEL, NIRAV B	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 01/23/2008	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/765,417

Applicant(s)

WATANABE ET AL.

Examiner

Nirav Patel

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 02 November 2007.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-63 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-63 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_

- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. Applicant's amendment filed on November 02, 2007 has been entered. Claims 1-63 are pending. Claims 10, 53-61 and 63 are also amended by the applicant.
2. The Office would like to notify the Applicant that there has been a change in Examiner to conduct the future examination and prosecution processes of the currently pending application.

### Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Y. Choi and S. Pack, "Fast Inter-AP Handoff Using Predictive Authentication Scheme in a Public Wireless Network." (hereafter "Choi") and in view of Faccin et al (US Patent No. 6,876,747).

C1. A method for handoff in a wireless communication network, comprising: generating a handoff encryption key [Page 1, Introduction, Lines 11-14.]; handing off a wireless terminal from a first access point to a second access point [Page 1, Introduction, Lines 11-14.]; and communicating data packets, between the second access point and the wireless terminal and authenticating the wireless terminal [Page 1, Introduction, Lines

11-14, page 6, 3.2 lines 8-15, page 7, Fig. 5, 6]. Choi teaches the re-authentication after handoff as shown in Fig. 6. Choi doesn't expressively mention communicating data packets encrypted with the handoff encryption key, between the second access point and the wireless terminal for immediate secured data transmission (i.e. secure data transmission during the handoff without perceivable interruption).

Faccin teaches communicating data packets encrypted with the handoff encryption key, between the second access point and the wireless terminal for immediate secured data transmission (secure data transmission during the handoff without perceivable interruption i.e. before the authentication of the wireless terminal) [col. 2 lines 1-16, Fig. 1, 5].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Faccin with Choi, since one would have been motivated to provide security mobility between two cellular systems [Faccin, col. 1 lines 9-10].

C2. The method according to claim 1, wherein the handoff encryption key is a handoff WEP (Wired Equivalent Privacy) key [Page 1, Introduction, Lines 11-14.].

C3. The method according to claim 1, wherein the handoff encryption key is generated by an authentication server [Page 1, Introduction, Lines 11-14.].

C4. The method according to claim 3, wherein the authentication server is an AAAH (Authentication, Authorization, and Accounting Home) server [Page 1, Introduction, Lines 15-20. Figure 5, "Home AAA Server."].

C5. The method according to claim 3, wherein the authentication server is an AAAF (Authentication, Authorization, and Accounting Foreign) server [Page 1, Introduction, Lines 15-20. Figure 5, "Gateway."].

C6. The method according to claim 3, wherein the handoff encryption key is generated according to IEEE 802.11 [Page 2, Introduction, Line 6.].

C7. The method according to claim 3, further comprising transmitting the handoff encryption key to the first and second access points [Page 2, Introduction, Lines 17-19.].

C8. The method according to claim 7, further comprising, at the first access point transmitting the handoff encryption key to the wireless terminal [Page 7, §3.2, Lines 4-6.].

C9. The method according to claim 8, further comprising, at the second access point decrypting data from the wireless terminal with the handoff encryption key [Figure 6.].

C10. The method according to claim 3, further comprising communicating handoff authentication messages between the wireless terminal and the second access points [Page 7, §3.2, Lines 7-11.].

C11. The method according to claim 10, further comprising encrypting the handoff authentication messages with the handoff encryption key [Page 7, §3.2, last sentence.].

Choi discloses generation of the handoff was only shown within the Authentication, Authorization and Accounting (AAA) server(s). Despite, moving the key generation functionality from the AAA server(s), home or foreign, to the access points (AP) by either a transmission of the algorithm itself and its associated parameters or simply the parameters (assuming the algorithm is already present within the AP) is obvious to anyone of ordinary skill in the art at the time the invention was made because both logical units (AAA server(s) and the APs) are logically equivalent with regards to key generation. Whether the AAA server generates the handoff key to be transmitted to the APs or the AAA server gives the algorithm to the APs in order to generate the keys does not change the patentable weight of the invention. Further, the board has found that the limitation of the "metallic wrapping," which is really a lining of the tube, presents no novel or unexpected result over the metallic connections used in the references. Use of such a means of electrical connection in lieu of those used in the references solves no stated problem and would be an obvious matter of design choice within the skill of the art. The same situation arises in digital implementations when a

system contains a plurality of logical units capable of the same functionality. Deciding whether one logical unit of a network system performs a specified functionality or another is an obvious matter of design choice. In other words, change of form or design without change of function is no more than choice of design that, in absence of new or unobvious result, falls within ken of one having ordinary skill in art and will not sustain patentability. *In re Launder*, 42 CCPA 886, 222 F.2d 371, 105 USPQ 446 (1955); *Flour City Architectural Metals v. Alpana Aluminum Products, Inc.*, 454 F. 2d 98, 172 USPQ 341 (8th Cir. 1972); *National Connector Corp. v. Malco Manufacturing Co.*, 392 F.2d 766, 157 USPQ 401 (8th Cir.) cert. denied, 393 U.S. 923, 159 USPQ 799 (1968).

The claims are addressed individually in light of the reference teaching the same functionality of the instant application, and moving said functionality between the AAA server(s) and access points having been deemed obvious:

C12. The method according to claim 1, wherein the handoff encryption key is generated by the first and second access points as a function of common handoff encryption key generation information from an authentication server [Transposing functionality from one logical unit to another to forgo network communication is well known in the art and deemed obvious, and key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification.].

C13. The method according to claim 1, further comprising, at the second access point, determining whether a packet received is encrypted by the handoff encryption key [Page 7, §3.2, last sentence. Also Figure 6.].

C14. The method according to claim 13, further comprising, at the second access point, decrypting a packet encrypted by the handoff encryption key [Rejected per claim 13.].

C15. The method according to claim 1, wherein the first access point and the second access point receive a common handoff authentication key generation process from an authentication server [Page 6, §3.2, Lines 12-14.].

C16. The method according to claim 15, further comprising: providing a secret parameter to a handoff encryption key generator associated with the first access point; providing an open parameter to the handoff encryption key generator associated with the first access point; and generating the handoff encryption key as a function of the secret parameter and the open parameter [Key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification.].

C17. The method according to claim 16, wherein the secret parameter comprises information about the authentication server [Key generation by parameters (MAC, IP



address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification.].

C18. The method according to claim 17, wherein the secret parameter comprises ID information of the authentication server and at least one common parameter of the authentication server [Key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification.].

C19. The method according to claim 16, wherein the open parameter comprises information about the first access point [Key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification.].

C20. The method according to claim 16, wherein the open parameter comprises information about the wireless terminal [Key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification.].

C21. The method according to claim 16, wherein the open parameter comprises the address of the first access point and the address of the wireless terminal [Key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use

of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification.].

C22. The method according to claim 16, further comprising transmitting the handoff encryption key from the first access point to the wireless terminal [Page 7, §3.2, Lines 4-6.].

C23. The method according to claim 16, further comprising, at the wireless terminal, transmitting to the second access point data encrypted by the handoff encryption key [Figure 6.].

C24. The method according to claim 16, further comprising, at the second access point, obtaining the address of the first access point [Page 2, Introduction, Lines 11-14.].

C25. The method according to claim 16, further comprising, at the second access point, obtaining the address of the wireless terminal [Key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "§3.3-4, pages 343-344, Protocol" for verification. Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification.].

C26. The method according to claim 16, further comprising, at the second access point, deriving the handoff encryption key according to the key generation process [Key

generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification.].

C27. The method according to claim 16, further comprising, at the second access point, decrypting data from the wireless terminal with the handoff encryption key [Figure 6.].

C28. A wireless communication network comprising: an authentication server operable to generate and transmit a handoff encryption key; a first access point, receiving the handoff encryption key; and a second access point, receiving the handoff encryption key from the authentication server and decrypting encrypted data from a wireless terminal before authentication of the wireless terminal is completed [Page 1, Introduction, Lines 11-14 and Page 7, §3.2, Lines 4-15.].

C29. The wireless communication network according to claim 28, wherein the handoff encryption key is a handoff WEP (Wired Equivalent Privacy) key [Rejected per claim 2.].

C30. The wireless communication network according to claim 28, wherein the authentication server is an AAAH (Authentication, Authorization, and Accounting Home) server [Rejected per claim 4.].

C31. The wireless communication network according to claim 28, wherein the authentication server is an AAAF (Authentication, Authorization, and Accounting Foreign) server [Rejected per claim 5.].

C32. The wireless communication network according to claim 28, wherein the handoff encryption key is generated according to IEEE 802.11 [Rejected per claim 6.].

C33. The wireless communication network according to claim 28, wherein the second access point communicates handoff authentication messages with the wireless terminal [Rejected per claim 10.].

C34. A wireless communication network comprising: an authentication server operable to generate and transmit handoff encryption key generation information; a first access point, generating a first handoff encryption key as a first function of the handoff encryption key generation information; and a second access point, generating a second handoff encryption key as a second function of the handoff encryption key generation information and decrypting encrypted data from a wireless terminal before authentication of the wireless terminal is completed [Rejected per claim 12.].

C35. The wireless communication network according to claim 34, wherein the handoff encryption key is a handoff WEP (Wired Equivalent Privacy) key [Rejected per claim 2.].

C36. The wireless communication network according to claim 34, wherein the authentication server is an AAAH (Authentication, Authorization, and Accounting Home) server [Rejected per claim 4.].

C37. The wireless communication network according to claim 36, wherein the AAAH server communicates with the first and second access points via an AAAF (Authentication, Authorization, and Accounting Foreign) server [Rejected per claim 2.].

C38. The wireless communication network according to claim 37, wherein the AAAF server communicates with the first and second access points via a router [Figure 5.].

C39. The wireless communication network according to claim 34, wherein the authentication server is an AAAF (Authentication, Authorization, and Accounting Foreign) server [Rejected per claim 5.].

C40. The wireless communication network according to claim 34, wherein the second access point communicates handoff authentication messages with the wireless terminal [Rejected per claim 10.].

C41. A wireless communication network comprising: an authentication server operable to generate and transmit a handoff encryption key generation secret parameter; a handoff encryption key generator, generating a handoff encryption key as a function of

the handoff encryption key generation secret parameter and an open parameter [The Examiner takes Official Notice that it is well known in the art to use a custom string (e.g., a 'secret parameter') to form a WEP key, known as "ASCII passphrases."]; a first access point, transmitting the handoff encryption key; and a second access point, deriving the handoff encryption key and decrypting encrypted data from a wireless terminal before authentication of the wireless terminal is completed [Rejected per claim 12.].

C42. The wireless communication network according to claim 41, wherein the secret parameter comprises information about the authentication server [Rejected per claim 17.].

C43. The wireless communication network according to claim 42, wherein the secret parameter comprises ID information of the authentication server and common parameter of the authentication server [Rejected per claim 18.].

C44. The wireless communication network according to claim 41, wherein the open parameter comprises information about the first access point [Rejected per claim 19.].

C45. The wireless communication network according to claim 41, wherein the open parameter comprises information about the wireless terminal [Rejected per claim 20.].

C46. The wireless communication network according to claim 41, wherein the open parameter for the first access point comprises the address of the first access point and the address of the wireless terminal [Rejected per claim 21.].

C47. The wireless communication network according to claim 41, wherein the second access point obtains the address of the first access point [Rejected per claim 24.].

C48. The wireless communication network according to claim 41, wherein the second access point obtains the address of the wireless terminal [Rejected per claim 25.].

C49. A wireless communication network comprising: a first authentication server operable to generate and transmit a first handoff encryption key; a second authentication server operable to generate and transmit a second handoff encryption key; a first access point, receiving the first handoff encryption key; and a second access point, receiving both the first handoff encryption key and the second handoff encryption key, and decrypting encrypted data from a wireless terminal before authentication of the wireless terminal is completed [Rejected per claim 1.].

C50. The wireless communication network according to claim 49, wherein the first authentication server is an AAAF (Authentication, Authorization, and Accounting Foreign) server [Rejected per claim 5.].

C51. The wireless communication network according to claim 49, wherein the first authentication server is an AAAH (Authentication, Authorization, and Accounting Home) server [Rejected per claim 4.].

C52. The wireless communication network according to claim 51, wherein the first authentication server communicates with the first and second access points via an AAAF (Authentication, Authorization, and Accounting Foreign) server [Figure 5.].

C53. A wireless access point comprising a memory which stores: instructions to receive a handoff encryption key generation secret parameter from an authentication server; instructions to receive a first packet from a wireless terminal, wherein the first packet includes an address of the wireless terminal; instructions to generate a handoff encryption key as a function of the handoff encryption key generation secret parameter and the address of the wireless terminal; and instructions to transmit the handoff encryption key to a wireless terminal [Rejected per claim 28 *and* 34.].

C54. The wireless access point according to claim 53, where the memory further stores: instructions to receive a second packet from the wireless terminal; instructions to decrypt data in the second packet with the handoff encryption key; and instructions to transmit the decrypted data [Rejected per claims 8 & 9.].



C55. A wireless access point comprising a memory which stores: instructions to receive a handoff encryption key from an authentication server; instructions to transmit the handoff encryption key to a first wireless terminal; instructions to receive data encrypted with the handoff encryption key from a second wireless terminal; instructions to decrypt the data with the handoff encryption key before authentication of the second wireless terminal is completed; and instructions to transmit the decrypted data [Rejected per claim 1-27].

C56. A wireless access point comprising a memory which stores: instructions to receive a handoff encryption key generation information from an authentication server; instructions to receive data from a wireless terminal; instructions to generate a handoff encryption key based on the handoff encryption key generation information and the data; instructions to decrypt the data with the handoff encryption key before authentication of the wireless terminal is completed; and instructions to transmit the decrypted data [Rejected per claim 28-40.].

C57. A handoff encryption key generator in a wireless communication network, comprising: an input to receive a handoff encryption key generation secret parameter; an input to receive an open parameter; and a generator for generating a handoff encryption key as a function of the handoff encryption key generation secret parameter and the open parameter [Rejected per claim 28-40.].

C58. The handoff encryption key generator according to claim 57, wherein the secret parameter comprises information about an authentication server [Rejected per claim 12.].

C59. The handoff encryption key generator according to claim 57, wherein the secret parameter comprises ID information of the authentication server and at least one common parameter of the authentication server [Rejected per claim 28-40.].

C60. The handoff encryption key generator according to claim 57, wherein the open parameter comprises information about an access point [Rejected per claim 28-40.].

C61. The handoff encryption key generator according to claim 57, wherein the open parameter comprises information about a wireless terminal [Rejected per claim 28-40.].

C62. The handoff encryption key generator according to claim 57, wherein the open parameter comprises the address of an access point and the address of a wireless terminal [Rejected per claim 28-40.].

C63. A wireless terminal in a wireless communication network, comprising a memory which stores: instructions to receive a handoff encryption key from a first access point; instructions to encrypt output data with the handoff encryption key; and instructions to

send the encrypted data to a second access point before authentication of the wireless terminal is completed [Rejected per claim 1-27.].

### Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 1-63 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-25 of copending Application No. 10/290,650. Although the conflicting claims are not identical, they are not patentably distinct from each other because both sets of claims are drawn

to composing handoff encryption keys for two access points of an IEEE 802.11 standard network for fast handoff. Both sets of claims (instant application's claims 1-27 and copending application's claims 1-25) match in order they are presented using the most recent set of amended claims within the copending application (dated 10/27/2005).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

#### **Response to Argument**

5. Applicant's arguments filed Nov. 02, 2007 have been fully considered. In view of applicant's argument that Choi does not disclose or suggest the claimed limitation "...immediate secure data transmission..... (i.e. allows data communication during the handoff without perceivable interruption", is found persuasive. Newly found reference by Faccin et al is used in combination with Choi as above. Faccin teaches the method and system for providing security mobility between two cellular systems. One or more cipher keys are generated. The traffic is handed off by the mobile device from the first cellular system to the second cellular system. The traffic between the mobile device and the second cellular system is encrypted using the one or more second ciphering keys. The ciphering of the traffic is maintained during handoff (i.e. allows data communication during the handoff without perceivable interruption). Therefore, the combination of Choi and Faccin teaches the claim limitation. See new ground of rejection above.

Examiner acknowledges the applicant's remark regarding the double patent rejection. Due to failure in submitting the terminal disclaimer for the provisional double patenting rejection, Examiner still maintains the Double patenting rejection.

### **Conclusion**

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Einola et al (US 7065340) – Arranging authentication and ciphering in mobile communication system

Kallio (US 2004/0014422) – Method and system for handovers using service description data

Heinonen et al (US 7103359) – Method and system for access point roaming

Rom (US 6360264) – Method and apparatus for maintaining connectivity of nodes in a wireless local area network

Norefors et al (US 6370380) – Method for secure handover

Vanderveen (US 2002/0197979) – Authentication system for mobile entities

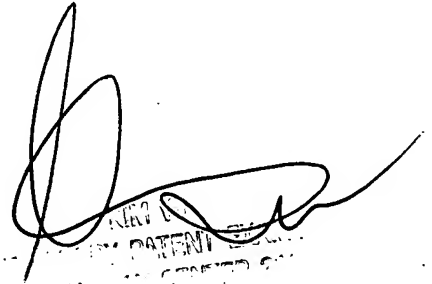
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

*NBP*

*1/18/08*



A handwritten signature in black ink, appearing to be 'NBP', is written over a faint, partially legible stamp. The stamp contains the words 'PATENT' and 'EXAMINER'.